

# All Mutually Unbiased Product Bases in Dimension Six

Daniel McNulty and Stefan Weigert  
 Department of Mathematics, University of York  
 York YO10 5DD, UK

dm575@york.ac.uk, stefan.weigert@york.ac.uk

24 March 2012

## Abstract

All mutually unbiased bases in dimension six consisting of product states only are constructed. Several continuous families of pairs and two triples of mutually unbiased product bases are found to exist but no quadruple. The exhaustive classification leads to a proof that a complete set of seven mutually unbiased bases, if it exists, cannot contain a triple of mutually unbiased product bases.

## 1 Introduction

Mutually unbiased (MU) bases [1–3] have attracted interest in recent years because their properties seem to depend dramatically on the dimension  $d$  of the quantum system in hand. If the dimension is given by a prime number  $p$ , the state space  $\mathbb{C}^p$  is known to accommodate a *complete* set of  $(p + 1)$  MU bases. Each of these bases consists of  $p$  orthonormal states  $|j_a\rangle \in \mathbb{C}^p$ , with constant overlap of  $1/p$  across different bases,

$$|\langle j_a | k_b \rangle|^2 = \frac{1}{p}(1 - \delta_{ab}) + \delta_{jk}\delta_{ab}, \quad j, k = 0 \dots p-1, \quad a, b = 0 \dots p. \quad (1)$$

Complete sets of MU bases also exist for quantum systems with dimension  $d = p^n$ , where  $n$  is a positive integer. However, for “composite” dimensions such as

$d \equiv d_1 d_2 \in \{6, 10, 12, \dots\}$  complete sets of MU bases seem to be absent. In spite of considerable numerical searches [4,5], computer-algebraic efforts [6,7], and numerical calculations with rigorous error bounds, only three MU bases have been found in dimension six, four less than the maximally allowed number [8]. Thus, the six-dimensional state space of a qubit-qutrit system appears to differ structurally from the state space of a pair of qubits ( $d = 4$ ) or a pair of qutrits ( $d = 9$ ).

One of the few known results in dimension  $d = 6$  is the impossibility to extend, by more than one further MU basis, the pair of MU bases consisting of the standard basis and its dual, the Fourier basis [6]. Thus, triples of MU bases are the largest sets to be found in this way. Another, more recent result [8] states that the Fourier family of Hadamard matrices together with the identity cannot be extended to a MU quadruple. These initial pairs, after non-local equivalence transformations, consist of *product* states only, a fact which has received little attention.

Upon reflection, it seems worthwhile to systematically study MU bases in composite dimensions which contain only product states. In the present paper we carry out a comprehensive study of MU product bases in dimensions six, complementing studies devoted to the entanglement structure of *complete* sets of MU bases [9–11].

More specifically, we will derive an exhaustive list of MU product bases in dimension six. The restriction to product states goes hand in hand with local equivalence transformations, or LETs, consisting of *local* (anti-) unitary transformations. We will find that in the space  $\mathbb{C}^2 \otimes \mathbb{C}^3$ , there is a considerable number of inequivalent product bases, a limited set of families of MU product *pairs* and just two *triples* of MU product bases. No larger MU product constellations exist. This result effectively limits the number of MU product bases contained in a hypothetical complete set of MU bases in dimension six.

The argument will unfold as follows. In Sec. 2 we introduce MU product bases, specify all local (anti-) unitary transformations which map a given set of MU product states to an equivalent one, and summarise relevant properties of MU bases in dimensions two and three. Then, in Sec. 3, we derive all inequivalent product bases in  $\mathbb{C}^4$  and  $\mathbb{C}^6$ . Sec. 4 has two results on product vectors required to be MU to certain given sets of MU product vectors. These results will be important tools to enumerate all pairs and triples of MU bases in dimension four (Sec. 5) and dimension six (Sec. 6). This classification allows us to conclude, as shown in Sec. 7, that no MU product triple can be part of a complete set of seven MU bases in  $d = 6$ . The final section summarises our findings.

Readers mainly interested in the results relevant to dimension six are advised to immediately proceed to Sec. 6 after having familiarized themselves with the concept

of mutually unbiased product bases presented in Sec. 2.

## 2 MU product bases

From now on, we will consider quantum systems consisting of two subsystems with prime dimensions  $p$  and  $q$ , where  $p \leq q$ . The state space of such a bipartite system is given by the Hilbert space  $\mathbb{C}^p \otimes \mathbb{C}^q$  of dimension  $d \equiv pq$ . Since  $q$  is a prime number, there is a complete set of MU bases of  $\mathbb{C}^q$ , and we will denote its  $q(q+1)$  states by

$$|J_b\rangle \in \mathbb{C}^q, \quad J = 0 \dots q-1, \quad b = 0 \dots q. \quad (2)$$

The  $q$  states  $\{|J_b\rangle\}$  form one orthonormal basis labelled by  $b$ , and states taken from two distinct bases are MU, in analogy to Eq. (1). Given complete sets of MU bases in  $\mathbb{C}^p$  and  $\mathbb{C}^q$ , respectively, we now construct  $(p+1)$  MU *product* bases of the space  $\mathbb{C}^p \otimes \mathbb{C}^q$ . To do so, we pair each MU basis of the space  $\mathbb{C}^p$  with a (different) basis of  $\mathbb{C}^q$  and, within each pair, we tensor each state of the first basis with a (different) state of the second one. This procedure results in  $pq(p+1)$  *product* states

$$|j_a\rangle \otimes |J_a\rangle \equiv |j_a, J_a\rangle, \quad (3)$$

forming  $(p+1)$  MU bases  $\{|j_a, J_a\rangle, a = 0 \dots p\}$  of the space  $\mathbb{C}^p \otimes \mathbb{C}^q$ . This is evident upon calculating the overlaps

$$|\langle j_a, J_a | k_b, K_b \rangle|^2 = |\langle j_a | k_b \rangle|^2 |\langle J_a | K_b \rangle|^2 = \begin{cases} \delta_{jk} \delta_{JK} & \text{if } a = b, \\ \frac{1}{pq} & \text{if } a \neq b, \end{cases} \quad (4)$$

which are the conditions for bases to be MU in a space of dimension  $pq$ .

One can construct MU product bases of the type given in Eq. (3) using Heisenberg-Weyl (HW) operators. In dimension  $p$ , with  $p$  prime, the HW cyclic shift (modulo  $p$ ) and phase operators  $X_p$  and  $Z_p$ , respectively, are defined as

$$X_p |j\rangle = |j+1\rangle \quad \text{and} \quad Z_p |j\rangle = \omega^j |j\rangle, \quad (5)$$

where  $\omega = e^{2\pi i/p}$  is a  $p^{\text{th}}$  root of unity and  $\{|j\rangle\}$  is the standard basis with  $j = 0 \dots p-1$ . Since  $p$  is prime, one can construct a complete set of  $(p+1)$  MU bases from the eigenbases of the operators  $X_p(Z_p)^\ell$  for  $0 \leq \ell \leq p-1$  [12].

For the composite dimension  $d = pq$ , we can build a set of  $(p+1)$  MU product bases of the Hilbert space  $\mathbb{C}^p \otimes \mathbb{C}^q$  with the operators  $X_p$  and  $Z_p$  acting on the space  $\mathbb{C}^p$ , and  $X_q$  and  $Z_q$  on the space  $\mathbb{C}^q$ . For example, the eigenbases of the operators  $X_p \otimes X_q$

and  $Z_p \otimes Z_q$  form two MU product bases, which we call a Heisenberg-Weyl pair. One can also construct HW bases with the operators  $X_{pq}$  and  $Z_{pq}$  on the space  $\mathbb{C}^{pq}$ , however, these do not necessarily form product bases. Since we are concerned with product bases in this paper, we define the HW operators on the space  $\mathbb{C}^p \otimes \mathbb{C}^q$  such that their eigenstates are product states. Note that we do not limit the construction of MU bases to the eigenbases of HW operators, i.e.  $\{|j_a, J_a\rangle\}$  in (3) can be *any* product basis.

Each basis  $\{|j_a, J_a\rangle\}$  is a *direct* product basis of the space  $\mathbb{C}^p \otimes \mathbb{C}^q$  since *each* state  $|j_a\rangle, j = 0 \dots p-1$ , of the  $a^{\text{th}}$  basis in  $\mathbb{C}^p$  is multiplied with *every* state  $|J_a\rangle, J = 0 \dots q-1$ , of the  $a^{\text{th}}$  basis of  $\mathbb{C}^q$ . Direct product bases are, however, only a subset among all product bases: *indirect* product bases [10] result if the states being tensored stem from more than one basis of the space  $\mathbb{C}^p$  (or  $\mathbb{C}^q$ ). The four states

$$\{|0_z, 0_z\rangle, |0_z, 1_z\rangle, |1_z, 0_x\rangle, |1_z, 1_x\rangle\} \quad (6)$$

provide a simple example of an *indirect* product basis in dimension four since two different bases of the second space,  $\{|j_z\rangle\}$  and  $\{|j_x\rangle\}$ , occur in the construction. The matrix representation of a *direct* product basis in dimension  $d = pq$  is given by the tensor product of two matrices, each representing a basis of the spaces  $\mathbb{C}^p$  and  $\mathbb{C}^q$ , respectively. The matrix representation of an *indirect* product basis cannot be written as a tensor product of two matrices.

Conceptually, the distinction between direct and indirect product bases is not linked to MU bases: instead of using  $\{|j_z\rangle\}$  and  $\{|j_x\rangle\}$  in (6) any other pair of bases of  $\mathbb{C}^2$  would also define an indirect product basis. Indirect product bases are important since they have been found to exhibit a degree of non-locality in the absence of entanglement [13].

In this paper, we will be concerned exclusively with product bases of the spaces  $\mathbb{C}^2 \otimes \mathbb{C}^2$  and  $\mathbb{C}^2 \otimes \mathbb{C}^3$ . To simplify the construction of all different MU product bases, we will now introduce equivalence relations which respect the structure of product states, followed by a brief reminder of the properties of MU bases in  $\mathbb{C}^2$  and  $\mathbb{C}^3$  following conventions used in [14].

## 2.1 Local equivalence transformations

Given a set of MU bases on the space  $\mathbb{C}^p$ , we obtain another set by applying one single unitary transformation to all states simultaneously. The scalar products between the states of the MU bases do not change under this transformation so that we deal

indeed with a second set of MU bases, factually *different* from the initial set but *equivalent* to it. By not distinguishing between equivalent MU bases, their enumeration is greatly simplified. When representing MU bases by Hadamard matrices, the concept of a standard (or dephased) form emerges naturally (see [15], for example). To enumerate all MU *product* bases it will be helpful not to distinguish those sets of MU product bases which can be transformed into each other by *local* equivalence transformations, or LETs, for short. LETs are defined by the requirement that they preserve the product structure of all states. If there is no LET transforming two given sets of MU product states into each other they will be called *locally inequivalent*, or just *inequivalent*. It may still be possible to transform them into each other by *non-local* transformations.

We now list all LETs for a bipartite quantum system with Hilbert space  $\mathbb{C}^p \otimes \mathbb{C}^q$ . Suppose we are given sets of  $(r + 1)$  MU bases  $\{\mathcal{B}_0, \mathcal{B}_1, \dots, \mathcal{B}_r\}$  that contain only product states. Explicitly, the  $\rho^{\text{th}}$  basis, with  $\rho = 0 \dots r$ , consists of  $d = pq$  product states  $|n_\rho, N_\rho\rangle$ ,  $n \equiv N \in \{1, 2, \dots, d\}$ , where  $|n_\rho\rangle \in \mathbb{C}^p$  and  $|N_\rho\rangle \in \mathbb{C}^q$ . Any combination of the following five operations maps the given set of MU bases into a locally equivalent set:

1. a *local unitary* transformation  $\hat{u} \otimes \hat{U}$  effecting

$$\mathcal{B}_\rho \rightarrow \mathcal{B}'_\rho = \hat{u} \otimes \hat{U} \mathcal{B}_\rho \equiv \left\{ \dots, |\hat{u}n_\rho\rangle \otimes |\hat{U}N_\rho\rangle, \dots \right\}, \quad (7)$$

which leaves invariant the value of all scalar products;

2. the multiplication of all states within a basis by possibly different *phase factors* such that

$$\mathcal{B}_\rho \rightarrow \mathcal{B}'_\rho = \left\{ \dots, e^{i\phi_n^p} |n_\rho, N_\rho\rangle, \dots \right\}; \quad (8)$$

these transformations exploit the fact that the overall phase of a quantum state has no physical significance and automatically drops out from the conditions defining MU bases. It is worth noting that a single phase factor  $e^{i\phi}$  can dephase *both* states of a product: let  $\phi \equiv \phi' + \phi''$  to find  $e^{i\phi} |n_\rho, N_\rho\rangle = (e^{i\phi'} |n_\rho\rangle) \otimes (e^{i\phi''} |N_\rho\rangle)$ ;

3. *permutations* of the product states within each basis; as an example, consider the permutation of states  $|n_\rho, N_\rho\rangle$  and  $|n'_\rho, N'_\rho\rangle$  in the  $\rho^{\text{th}}$  basis

$$\left\{ \dots, |n_\rho, N_\rho\rangle, \dots, |n'_\rho, N'_\rho\rangle, \dots \right\} \longrightarrow \left\{ \dots, |n'_\rho, N'_\rho\rangle, \dots, |n_\rho, N_\rho\rangle, \dots \right\}, \quad (9)$$

which amounts to relabelling the elements within each basis;

4. the *local complex conjugations*  $\hat{k} \otimes \hat{I}$  and  $\hat{I} \otimes \hat{K}$  (anti-unitary operations defined with respect to the standard bases in  $\mathbb{C}^p$  and  $\mathbb{C}^q$ , respectively), and thus their product  $\hat{k} \otimes \hat{K}$ ; for example, applying  $\hat{k} \otimes \hat{I}$

$$\mathcal{B}_\rho \rightarrow \mathcal{B}'_\rho = \left\{ \dots, |n_\rho^*, N_\rho\rangle, \dots \right\}, \quad (10)$$

swaps all scalar products resulting from the first factors without changing their numerical values;

5. *pairwise exchanges* of two bases, which amounts to relabelling the bases.

We now briefly discuss some important properties of LETs. First, they represent a true subset of all equivalence transformations in a space of dimension  $pq$ : no LET maps an indirect product basis to a direct one while a general unitary equivalence transformation can send any orthonormal basis to any other. Second, we will find indirect product bases which cannot be transformed into each other by LETs, i.e. *locally inequivalent* product bases. As a result, the idea of a *unique* standard or dephased form of MU bases is less straightforward for MU product bases. We define a standard form in the following way: the first basis  $\mathcal{B}_0$ , be it direct or indirect, contains the states  $\{|j_z\rangle\}$  of the space  $\mathbb{C}^p$  and the states  $\{|J_z\rangle\}$  of the space  $\mathbb{C}^q$ ; the second basis  $\mathcal{B}_1$  contains the state  $|0_x, 0_x\rangle$ , and all other states in the remaining bases are dephased using the transformation defined in (8). Superficially, LETs remind one of local operations with classical communication, or LOCCs [16]. However, the presence of anti-unitary operations rather suggests a link with Wigner's theorem about symmetry transformations leaving transition probabilities invariant [17], for the special case of a universe populated with product states only. Finally, it is straightforward to generalise LETs to  $n$ -partite systems residing in product states only.

It is often convenient to represent an MU product basis in  $\mathbb{C}^{pq}$  as a complex Hadamard matrix of dimension  $(pq \times pq)$ , with each product state corresponding to one column. The bases  $\{\mathcal{B}_0, \mathcal{B}_1, \dots, \mathcal{B}_r\}$  then turn into a set of  $(r+1)$  matrices, on which the five transformations above act in the following way. The first LET is a *local unitary*, given by the Kronecker product of two unitary matrices, applied to all matrices from the left; the second LET corresponds to *diagonal unitary* transformations acting from the right; *unitary permutation matrices* acting from the right implement the third type of LET, while the effect of the *local complex conjugations* must be worked out by writing down each product state individually.

## 2.2 MU bases in dimensions two and three

Given a pair of MU bases in the vector space  $\mathbb{C}^2$ , we can always map the first basis to the standard basis  $\{|j_z\rangle\}$  by a suitable unitary transformation  $\hat{u} \in SU(2)$ . Being MU to the first basis, the states of the second basis now must have the form

$$|a\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle + e^{i\lambda}|1_z\rangle) \equiv \hat{r}_\lambda|+\rangle, \quad |a^\dagger\rangle = \hat{r}_\lambda|-\rangle, \quad (11)$$

where  $\{|\pm\rangle\} \equiv \{|j_x\rangle\}$  is the  $x$ -eigenbasis, and the operator  $\hat{r}_\lambda, \lambda \in [0, \pi)$ , represents a rotation by an angle  $\lambda$  about the  $z$ -axis. Since any such rotation leaves the standard basis  $\{|j_z\rangle\}$  unchanged, the second MU basis can be transformed into  $\{|j_x\rangle\}$ . The matrix representation of the resulting pair of MU bases reads

$$\{I; F_2\} \equiv \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\}. \quad (12)$$

All other pairs of MU bases of the space  $\mathbb{C}^2$  are, in fact, equivalent to this one. A third basis MU to these two bases consists of the states given in Eq. (11) if  $\lambda = \pm\pi/2$ , producing  $\{|j_y\rangle\}$ . Thus, all pairs of MU bases in  $\mathbb{C}^2$  are equivalent to  $\{|j_z\rangle; |j_x\rangle\}$ , and all triples are equivalent to  $\{|j_z\rangle; |j_x\rangle; |j_y\rangle\}$ , as is well known.

In dimension three, one of two given MU bases can always be mapped to the standard basis  $\{|J_z\rangle, J = 0, 1, 2\}$ , so that the second basis consists of states of the form

$$|A\rangle = \frac{1}{\sqrt{3}}(|0_z\rangle + e^{i\xi}|1_z\rangle + e^{i\eta}|2_z\rangle), \quad \xi, \eta \in [0, 2\pi), \quad (13)$$

exploiting the fact that the overall phase of a quantum state has no physical meaning. One can construct three states of this form which are pairwise orthogonal: writing

$$|A^\perp\rangle = \frac{1}{\sqrt{3}}(|0_z\rangle + \gamma e^{i\xi}|1_z\rangle + \delta e^{i\eta}|2_z\rangle), \quad |\gamma| = |\delta| = 1, \quad (14)$$

the condition  $\langle A | A^\perp \rangle = 0$  implies  $\gamma + \delta = -1$ . A geometric argument in the complex plane implies either  $\gamma = \omega$  and  $\delta = \omega^2$ , or  $\gamma = \omega^2$  and  $\delta = \omega$ , where  $\omega = e^{2\pi i/3}$  is a third root of unity. We denote the resulting basis by

$$\{|A\rangle, |A^\perp\rangle, |A^\perp\rangle\} = \{\hat{R}_{\xi,\eta}|J_x\rangle\}, \quad (15)$$

where the triple  $\{|J_x\rangle\} \equiv \{|J_x\rangle, J = 0, 1, 2\}$  consists of the eigenstates of the shift operator  $\hat{X}_3$ , and the operator  $\hat{R}_{\xi,\eta}$  is diagonal in the  $z$ -basis such that  $|A\rangle \equiv \hat{R}_{\xi,\eta}|0_x\rangle$ , cf. Eq. (13). The free parameters  $\xi, \eta$  in the pairs of MU bases  $\{|J_z\rangle; \hat{R}_{\xi,\eta}|J_x\rangle\}$  can be removed by a suitable redefinition of the phases of the states in the standard

basis  $\{|J_z\rangle\}$ . Thus, all pairs of MU bases of  $\mathbb{C}^3$  are equivalent to the pair  $\{|J_z\rangle; |J_x\rangle\}$  which may be represented by

$$\{I; F_3\} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \right\}, \quad (16)$$

where  $F_3 \equiv H_x$  is the Fourier matrix in  $\mathbb{C}^3$ . Note that two more orthonormal bases of states MU to the pair  $\{|J_z\rangle; |J_x\rangle\}$  emerge if one sets either  $e^{i\xi} = e^{i\eta} \equiv \omega$  or  $e^{i\xi} = e^{i\eta} \equiv \omega^2$  in Eq. (15). We will denote these bases by  $\{|J_y\rangle\}$  and  $\{|J_w\rangle\}$ , respectively, and their matrix representations are given by

$$H_y = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix}, \quad H_w = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix}, \quad (17)$$

which are also MU with respect to each other. The matrices  $H_x, H_y$  and  $H_w$  are complex  $(3 \times 3)$  Hadamard matrices, i.e. they are unitary and the moduli of all their entries are equal to  $1/\sqrt{3}$ .

Two *triples* of MU bases now result from adding either  $\{|J_y\rangle\}$  or  $\{|J_w\rangle\}$  to the pair  $\{|J_z\rangle; |J_x\rangle\}$ . These triples are equivalent to each other as follows from taking the complex conjugate (defined in the  $z$ -basis) of the triple  $\{|J_z\rangle; |J_x\rangle; |J_y\rangle\}$ : the complex conjugation only affects the ordering of states within  $\{|J_x\rangle\}$  while  $\{|J_y\rangle\}$  turns into  $\{|J_w\rangle\}$ . Thus we conclude that the triples are indeed equivalent which we express formally by writing

$$\{|J_z\rangle; |J_x\rangle; |J_y\rangle\} \sim \{|J_z\rangle; |J_x\rangle; |J_w\rangle\}. \quad (18)$$

Consequently, all MU triples are equivalent to the triple  $\{|J_z\rangle; |J_x\rangle; |J_y\rangle\}$ , and the complete set of four MU bases in  $\mathbb{C}^3$  is also unique, as is well known.

### 3 Constructing product bases in dimensions four and six

The first step towards an exhaustive list of pairs and triples of MU product bases in dimension six is to construct all locally inequivalent product bases in  $\mathbb{C}^2 \otimes \mathbb{C}^3$ . Once these are known, the requirement of any two such bases to be MU will impose further constraints. It will be helpful to initially carry out this construction in dimension four. Thus, we will first derive all inequivalent product bases of the space  $\mathbb{C}^2 \otimes \mathbb{C}^2$ , followed by a similar construction for a six-dimensional space.



### 3.1 All product bases in $d = 4$

We now show that each product basis in  $d = 4$  is equivalent either to the standard *direct* product basis or to a member of two families of *indirect* product bases, each depending on two real parameters. Any (orthonormal) product basis in the space  $\mathbb{C}^2 \otimes \mathbb{C}^2$  must have the form

$$\left\{ |\psi_1, \phi_1\rangle, |\psi_2, \phi_2\rangle, |\psi_3, \phi_3\rangle, |\psi_4, \phi_4\rangle \right\}, \quad (19)$$

where  $|\psi_n\rangle, |\phi_n\rangle \in \mathbb{C}^2$  for  $n = 1 \dots 4$ . The conditions

$$\langle \psi_n, \phi_n | \psi_{n'}, \phi_{n'} \rangle = \langle \psi_n | \psi_{n'} \rangle \langle \phi_n | \phi_{n'} \rangle = \delta_{nn'}, \quad n, n' = 1 \dots 4, \quad (20)$$

imply that at least two states of the first factor must be orthogonal. However, no three orthogonal states exist in  $\mathbb{C}^2$ , so that upon calling  $|\psi_1\rangle \equiv |a\rangle$  we must have

$$\left\{ |a, \phi_1\rangle, |a^\perp, \phi_2\rangle, |\psi_3, \phi_3\rangle, |\psi_4, \phi_4\rangle \right\}, \quad (21)$$

with  $|\psi_2\rangle = |a^\perp\rangle$  being the unique state orthogonal to  $|a\rangle$ . Now we need to consider two separate cases: we can have either  $|\psi_3\rangle = |a\rangle$  (or, equivalently,  $|\psi_3\rangle = |a^\perp\rangle$ ) or  $|\psi_3\rangle = |b\rangle$  such that  $0 < |\langle a | b \rangle| < 1$ , meaning that the state  $|b\rangle$  is neither a multiple of the state  $|a\rangle$  nor orthogonal to it; we call such a vector  $|b\rangle$  *skew* to  $|a\rangle$ .

By a simple argument using the restrictions imposed by the orthogonality conditions, one finds that three different bases result:

$$\mathcal{B}_0 = \left\{ |a, A\rangle, |a, A^\perp\rangle, |a^\perp, A\rangle, |a^\perp, A^\perp\rangle \right\}, \quad (22)$$

$$\mathcal{B}_1 = \left\{ |a, A\rangle, |a, A^\perp\rangle, |a^\perp, B\rangle, |a^\perp, B^\perp\rangle \right\}, \quad (23)$$

$$\mathcal{B}_2 = \left\{ |a, A\rangle, |a^\perp, A\rangle, |b, A^\perp\rangle, |b^\perp, A^\perp\rangle \right\}. \quad (24)$$

The basis  $\mathcal{B}_0$  is a direct product basis while the bases  $\mathcal{B}_1$  and  $\mathcal{B}_2$  are not. After performing suitable LETs, we can thus summarise the complete list of product bases in dimension four as follows.

**Lemma 1.** *Any orthonormal product basis of the space  $\mathbb{C}^2 \otimes \mathbb{C}^2$  is equivalent to a member of one of the families*

$$\begin{aligned} \mathcal{I}_0 &= \{|j_z, k_z\rangle\}, \\ \mathcal{I}_1 &= \{|0_z, k_z\rangle, |1_z, \hat{u}k_z\rangle\}, \\ \mathcal{I}_2 &= \{|j_z, 0_z\rangle, |\hat{v}j_z, 1_z\rangle\}, \end{aligned} \quad (25)$$

where the operators  $\hat{u}, \hat{v} \in SU(2)$  act on the space  $\mathbb{C}^2$  such that the states  $|0_z\rangle$  and  $\hat{u}|0_z\rangle$ , as well as the states  $|0_z\rangle$  and  $\hat{v}|0_z\rangle$ , are skew.

Note that the parameters on which the operators depend have been chosen in such a way that no product basis occurs more than once. A number of LETs (cf Sec. 2.1) have been used to bring the bases into the form given in the lemma. The basis  $\mathcal{B}_0$  in (22) has been mapped to  $\mathcal{I}_0$  by means of a transformation  $\hat{u}_1 \otimes \hat{u}_2$  such that  $\hat{u}_1$  maps the pair of states  $\{|a\rangle, |a^\perp\rangle\}$  to the standard basis  $\{|j_z\rangle\}$  of  $\mathbb{C}^2$ , and  $\hat{u}_2$  is defined analogously. Thus, the bases  $\mathcal{B}_0$  and  $\mathcal{I}_0$  are equivalent to each other. We apply a similar transformation to the basis  $\mathcal{B}_1$  in (23) mapping two of the bases to the standard basis. The freedom to choose a third basis, associated with the pair  $\{|B\rangle, |B^\perp\rangle\}$ , is represented in  $\mathcal{I}_1$  by the undetermined unitary operator  $\hat{u}$  acting on the standard basis. The same reasoning brings  $\mathcal{B}_2$  into the form (25) except that the roles of the two spaces are swapped. Since a complex conjugation reflects points on the Bloch sphere about the  $xz$ -plane, only half of all the unitaries  $\hat{u}$  (and  $\hat{v}$ ) need to be considered in Lemma 1. In other words, the bases associated with the unitaries  $\hat{u}$  and  $\hat{u}^*$ , given by the complex conjugate of the matrix representing  $\hat{u}$  in the  $z$ -basis, coincide.

The symmetry of the space  $\mathbb{C}^2 \otimes \mathbb{C}^2$  is reflected in the fact that we found two bases  $\mathcal{I}_1$  and  $\mathcal{I}_2$  which are identical except for the order of the factors. If we stick with the idea that LETs dictate whether two product bases are equivalent to each other, we need to consider these bases as inequivalent. Thus, the complete set of product bases consists of two families each of which depends on two parameters due to the  $SU(2)$ -transformations  $\hat{u}$  and  $\hat{v}$ . Not all three parameters of a transformation in  $SU(2)$  are relevant since the overall phase of quantum states is physically irrelevant: each pair of opposite points on the Bloch sphere defines an orthonormal basis of  $\mathbb{C}^2$  so that the set of all bases depends on only two real parameters. Note that the sets  $\mathcal{I}_1$  and  $\mathcal{I}_2$  of Lemma 1 are both connected to the product basis  $\mathcal{I}_0$ .

The symmetry becomes particularly obvious if we represent the bases of Lemma 1 by quantum circuits. The idea is to visualise the operation needed to map the states of the standard product basis  $\mathcal{I}_0$  into the desired product basis by means of a quantum gate. This is always possible since any two orthonormal bases are connected by a unitary operation. Obviously, the trivial gate, described by the identity  $\hat{I}$ , maps the four vectors of the standard product basis to itself. Fig. (1) shows that (non-local) controlled- $\hat{u}$  and controlled- $\hat{v}$  gates are required to output the bases  $\mathcal{I}_1$  and  $\mathcal{I}_2$ , respectively. As expected, the two circuits are identical upon swapping the qubits.



**Figure 1:** Two quantum circuits to create the product bases  $\mathcal{I}_1$  and  $\mathcal{I}_2$ , respectively; the unitaries  $\hat{u}$  and  $\hat{v}$  only act on the target qubit if the control qubit is in the state  $|1_z\rangle$ .

### 3.2 All product bases in $d = 6$

To construct all product bases in dimension six we use the same method as in dimension four. Any product basis in the space  $\mathbb{C}^2 \otimes \mathbb{C}^3$  takes the form

$$\left\{ |\psi_1, \Psi_1\rangle, |\psi_2, \Psi_2\rangle, |\psi_3, \Psi_3\rangle, |\psi_4, \Psi_4\rangle, |\psi_5, \Psi_5\rangle, |\psi_6, \Psi_6\rangle \right\}, \quad (26)$$

with states  $|\psi_n\rangle \in \mathbb{C}^2$  and  $|\Psi_n\rangle \in \mathbb{C}^3$  for  $n = 1 \dots 6$ , satisfying the orthogonality conditions

$$\langle \psi_n, \Psi_n | \psi_{n'}, \Psi_{n'} \rangle = \langle \psi_n | \psi_{n'} \rangle \langle \Psi_n | \Psi_{n'} \rangle = \delta_{nn'}, \quad n, n' = 1 \dots 6. \quad (27)$$

The states  $|\psi_n\rangle, n = 1 \dots 6$ , in (26) must contain at least *two* (not necessarily different) pairs of orthogonal states. If they do not, the orthogonality conditions require *four* orthogonal states in  $\mathbb{C}^3$ , which do not exist. In fact, the remaining two states in  $\mathbb{C}^2$  must also be orthogonal, which implies that the product bases of  $\mathbb{C}^6$  will come in three flavours. The states  $|\psi_n\rangle, n = 1 \dots 6$ , fall into three pairs of states consisting of either three, two, or only one pair of orthonormal bases. The following lemma summarises the results of the detailed arguments given in Appendix A.

**Lemma 2.** *Any orthonormal product basis of the space  $\mathbb{C}^2 \otimes \mathbb{C}^3$  is equivalent to a member of one of the families*

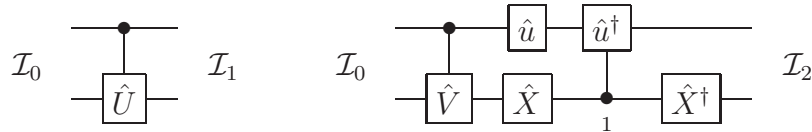
$$\begin{aligned} \mathcal{I}_0 &= \{|j_z, J_z\rangle\}, \\ \mathcal{I}_1 &= \{|0_z, J_z\rangle, |1_z, \hat{U}J_z\rangle\}, \\ \mathcal{I}_2 &= \{|j_z, 0_z\rangle, |\hat{u}0_z, 1_z\rangle, |\hat{u}0_z, 2_z\rangle, |\hat{u}1_z, \hat{V}1_z\rangle, |\hat{u}1_z, \hat{V}2_z\rangle\}, \\ \mathcal{I}_3 &= \{|j_z, 0_z\rangle, |\hat{v}j_z, 1_z\rangle, |\hat{v}j_z, 2_z\rangle\}, \end{aligned} \quad (28)$$

with  $j = 0, 1$  and  $J = 0, 1, 2$ ; the operators  $\hat{u}, \hat{v}, \hat{w} \in SU(2)$  and  $\hat{U}, \hat{V} \in SU(3)$  act on  $\mathbb{C}^2$  and  $\mathbb{C}^3$ , respectively, with  $\hat{V}$  leaving the state  $|0_z\rangle$  invariant; the parameters of the operators  $\hat{u}, \dots, \hat{V}$  are chosen in such a way that no product basis occurs more than once.

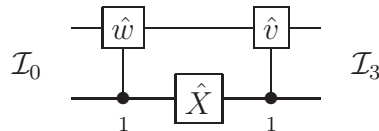
Without any restrictions on the five unitary operators  $\hat{u}, \dots, \hat{V}$  some product bases would occur more than once in this list. For example, if  $\hat{U} \equiv \hat{I}$ , the basis  $\mathcal{I}_1$  turns

into  $\mathcal{I}_0$ ; similarly, the bases associated with  $\hat{U}$  and  $\hat{U}^*$  are identical. We could remove such multiple occurrences by appropriately restricting the unitary operators but it is rather cumbersome to do so and not particularly informative.

Compared to dimension four, the number of families of indirect product bases have increased, and they contain transformations generated by elements of the group  $SU(3)$ . Clearly, there is no scope for symmetry under exchanging the two spaces of the product  $\mathbb{C}^2 \otimes \mathbb{C}^3$ . The families  $\mathcal{I}_1$  to  $\mathcal{I}_3$  each depend on a number of free parameters:  $\mathcal{I}_1$  has six free parameters due to the unitary  $\hat{U}$ ; two free parameters are associated with each  $SU(2)$ -transformation present in  $\mathcal{I}_3$ , while  $\mathcal{I}_2$  is a five-parameter family – the transformations due to  $\hat{V}$ , which is effectively an  $SU(2)$ -transformation, brings not only two but *three* parameters because the overall phase of the states in the two-dimensional subspace spanned by  $|1_z\rangle$  and  $|2_z\rangle$  does *not* drop out. Figs. (2) and (3) show quantum circuits to generate the inequivalent product bases in dimension six.



**Figure 2:** Quantum circuits for a qubit (upper wire) and qutrit (lower wire) to create the bases  $\mathcal{I}_1$  and  $\mathcal{I}_2$ , respectively; the controlled- $\hat{U}$  and controlled- $\hat{V}$  gate act on the qutrit only if the control qubit is in the state  $|1_z\rangle$ ; the unitary  $\hat{u}^\dagger$ , the adjoint of  $\hat{u}$ , acts on the qubit only when the control qutrit is in the state  $|1_z\rangle$ ; and the operator  $\hat{X}$  acts as a shift on the standard basis of  $\mathbb{C}^3$ .



**Figure 3:** A quantum circuit for a qubit (upper wire) and qutrit (lower wire) to create the basis  $\mathcal{I}_3$ ; the unitaries  $\hat{v}$  and  $\hat{w}$  act on the qubit only if the control qutrit is in the state  $|1_z\rangle$ , and the operator  $\hat{X}$  acts as a shift on the standard basis of  $\mathbb{C}^3$ .

## 4 Adding MU product states to sets of orthogonal product vectors

In this section we derive a theorem which will play a crucial role in the construction of *all* pairs and triples of MU product bases in dimension four and six. This theorem

is inspired by a constraint on two *direct* product bases to be MU, obtained in [10]:

**Lemma.** *Two [direct] product bases  $\{|j_a, J_a\rangle\}$  and  $\{|k_b, K_b\rangle\}$  in dimension  $d = pq$  are MU if and only if  $|j_a\rangle$  is MU to  $|k_b\rangle$  in dimension  $p$  and  $|J_a\rangle$  is MU to  $|K_b\rangle$  in dimension  $q$ .*

This result does not cover *indirect* bases. To (partly) remedy this shortcoming, we will present two different ways to generalise this Lemma. Firstly, we find a constraint on each product vector if it is to be MU to a specific set of product vectors; this result is obtained for spaces of arbitrary composite dimension  $d = pq$ . Secondly, we derive constraints on a product vector required to be MU to *any* (direct or indirect) given product basis of the spaces  $\mathbb{C}^4$  or  $\mathbb{C}^6$ .

Consider  $p$  product states  $\{|\psi_i, \Psi\rangle, i = 1 \dots p\}$  with an orthonormal basis  $\{|\psi_i\rangle, i = 1 \dots p\}$  of the space  $\mathbb{C}^p$ , and with  $|\Psi\rangle \in \mathbb{C}^q$ . After swapping the two factors in Eq. (6), the product basis  $\{|j_z, 0_z\rangle, |j_x, 1_z\rangle\}$ , for example, is seen to consist of two sets of this form. We find that only particular product states can be MU to such sets of product states.

**Lemma 3.** *The product state  $|\phi, \Phi\rangle$  in dimension  $d = pq$  is MU to the set of orthogonal product states  $\{|\psi_i, \Psi\rangle, i = 1 \dots p\}$  if and only if  $|\phi\rangle$  is MU to  $|\psi_i\rangle \in \mathbb{C}^p$  and  $|\Phi\rangle$  is MU to  $|\Psi\rangle \in \mathbb{C}^q$ .*

If  $|\langle\psi_i|\phi\rangle|^2 = 1/p$  and  $|\langle\Psi|\Phi\rangle|^2 = 1/q$ , then the product states are indeed MU in the space  $\mathbb{C}^{pq}$  since it follows that  $|\langle\psi_i, \Psi|\phi, \Phi\rangle|^2 = |\langle\psi_i|\phi\rangle|^2 |\langle\Psi|\Phi\rangle|^2 = 1/pq$ . To prove the converse, we assume the product states are MU,  $|\langle\psi_i, \Psi|\phi, \Phi\rangle|^2 = 1/pq$ . Summing over  $i = 1 \dots p$ , we obtain  $|\langle\Psi|\Phi\rangle|^2 = 1/q$  upon using the completeness relation  $\sum_i |\langle\psi_i|\phi\rangle|^2 = 1$ . This result immediately implies that  $|\langle\psi_i|\phi\rangle|^2 = 1/p, i = 1 \dots p$ , also holds.

Note that one can swap the roles of the factors in the tensor product. Then Lemma 3 restricts the form of any product state which is MU to a set of  $q$  orthogonal states  $\{|\psi, \Psi_i\rangle, i = 1 \dots q\}$  with an orthonormal basis  $\{|\Psi_i\rangle, i = 1 \dots q\}$  of the space  $\mathbb{C}^q$ , and with  $|\psi\rangle \in \mathbb{C}^p$ .

This result covers the Lemma given at the beginning of this section. To see this, group the basis  $\{|j_a, J_a\rangle\}$  into  $q$  sets of  $p$  orthonormal vectors  $\{|j_a, 1_a\rangle\}, \{|j_a, 2_a\rangle\} \dots \{|j_a, q_a\rangle\}$ ; then, by Lemma 3, any product state  $|\phi, \Phi\rangle$  is mutually unbiased to each set of vectors if and only if the state  $|\phi\rangle$  is MU to all states  $|j_a\rangle$ , and the state  $|\Phi\rangle$  is MU to all states  $|J_a\rangle$ . By replacing the state  $|\phi, \Phi\rangle$  with a vector from the basis  $\{|k_a, K_a\rangle\}$  and repeating the argument for all states in this basis, one arrives at the Lemma for *direct* product bases.

The following generalisation uses the fact that we know all direct and indirect product bases in dimensions four and six.

**Theorem 1.** *The product state  $|\phi, \Phi\rangle \in \mathbb{C}^d$ ,  $d \equiv pq \leq 6$ , is MU to the product basis  $\{|\psi_i, \Psi_i\rangle\}$  with  $i = 1 \dots pq$ , if and only if  $|\phi\rangle$  is MU to  $|\psi_i\rangle \in \mathbb{C}^p$  and  $|\Phi\rangle$  is MU to  $|\Psi_i\rangle \in \mathbb{C}^q$ .*

We prove this statement by considering the cases  $d = 4$  and  $d = 6$  separately:

- $d = 4$ : All product bases in dimension four are given by the bases  $\mathcal{I}_0, \mathcal{I}_1$  and  $\mathcal{I}_2$ , collected in Lemma 1. Each of these bases can be divided into groups of states of the form  $\{|\psi_j, \Psi\rangle, j = 1, 2\}$ , or  $\{|\psi, \Psi_j\rangle, j = 1, 2\}$ . Thus, Theorem 1 follows immediately from Lemma 3.

- $d = 6$ : It is sufficient to consider the four families of bases given in Lemma 2. Each of the bases  $\mathcal{I}_0, \mathcal{I}_1$  and  $\mathcal{I}_3$  can be split into sets of the form required to apply Lemma 3; thus, Theorem 1 holds for these bases. To complete the proof, we need to consider the basis  $\mathcal{I}_2$  which has no such decomposition. To begin, suppose that the basis  $\mathcal{I}_2$  is MU to the state  $|\phi, \Phi\rangle$ . According to Lemma 3 this state is MU to the pair  $\{|j_z, 0_z\rangle\}$  if both  $|\langle\phi|0_z\rangle|^2 = |\langle\phi|1_z\rangle|^2 = 1/2$  and  $|\langle\Phi|0_z\rangle|^2 = 1/3$  hold. The state  $|\phi, \Phi\rangle$  also needs to satisfy

$$|\langle\phi|\hat{u}0_z\rangle|^2|\langle\Phi|1_z\rangle|^2 = |\langle\phi|\hat{u}0_z\rangle|^2|\langle\Phi|2_z\rangle|^2 = \frac{1}{6}; \quad (29)$$

adding these two constraints we find

$$|\langle\phi|\hat{u}0_z\rangle|^2 \left( |\langle\Phi|1_z\rangle|^2 + |\langle\Phi|2_z\rangle|^2 \right) = \frac{1}{3}. \quad (30)$$

Using  $\sum_J |\langle\Phi|J_z\rangle|^2 = 1$ , i.e. the completeness relation of the basis  $\{|J_z\rangle\}$ , and  $|\langle\Phi|0_z\rangle|^2 = 1/3$ , we find that  $|\langle\Phi|1_z\rangle|^2 + |\langle\Phi|2_z\rangle|^2 = 2/3$ . Substituting this identity into (30) leaves us with  $|\langle\phi|\hat{u}0_z\rangle|^2 = 1/2$ , so that  $|\langle\Phi|1_z\rangle|^2 = |\langle\Phi|2_z\rangle|^2 = 1/3$  as well. A similar argument applied to the pair  $\{|\hat{u}1_z, \hat{V}1_z\rangle, |\hat{u}1_z, \hat{V}2_z\rangle\}$  shows that indeed  $|\langle\phi|\hat{u}1_z\rangle|^2 = 1/2$  and  $|\langle\Phi|\hat{V}1_z\rangle|^2 = |\langle\Phi|\hat{V}2_z\rangle|^2 = 1/3$ , which confirms that the state  $|\phi, \Phi\rangle$  is of the desired form. The *converse* direction of the statement is straightforward.

We conjecture Theorem 1 to hold for *all* product dimensions  $d \equiv pq$ , i.e.  $d = 4, 6, 9, 10, \dots$ . However, a proof similar to the one for  $d = 4, 6$ , would rely on the structure of all product bases in composite dimensions  $d > 6$  – which is not known to us.

## 5 MU product bases in dimension four

### 5.1 All pairs of MU product bases

To construct *pairs* of MU product bases in the space  $\mathbb{C}^4$ , we check all possibilities to form MU pairs of the product bases displayed in Lemma 1 of Sec. 3.1. We find two families of locally inequivalent MU product bases given in Proposition 1 below. The derivation of Proposition 1 relies on a technique also used for the six-dimensional case presented in Appendix B.

**Proposition 1.** *Any pair of MU product bases in the space  $\mathbb{C}^2 \otimes \mathbb{C}^2$  is equivalent to a member of the families*

$$\begin{aligned}\mathcal{P}_0^{(4)} &\equiv \{|j_z, k_z\rangle; |j_x, k_x\rangle\}, \\ \mathcal{P}_1^{(4)} &\equiv \{|0_z, k_z\rangle, |1_z, \hat{s}_\mu k_z\rangle; |j_x, 0_x\rangle, |\hat{r}_\nu j_x, 1_x\rangle\},\end{aligned}\tag{31}$$

where  $j, k = 0, 1$ , and the unitary operator  $\hat{r}_\nu$  rotates the basis  $\{|j_x\rangle\} \equiv \{|k_x\rangle\} \equiv \{|\pm\rangle\}$  into the  $xy$ -plane according to  $\hat{r}_\nu|\pm\rangle = (|0_z\rangle \pm e^{i\nu}|1_z\rangle)/\sqrt{2}$  for  $\nu \in (0, \pi)$ ; the operator  $\hat{s}_\mu$  generates rotations about the  $x$ -axis, i.e.  $\hat{s}_\mu|k_z\rangle = (|0_x\rangle + (-1)^{k_z}e^{i\mu}|1_x\rangle)/\sqrt{2}$  for  $\mu \in [0, \pi)$ .

The pair  $\mathcal{P}_0^{(4)}$  is the Heisenberg-Weyl pair consisting of two direct product bases. The pair of MU bases  $\mathcal{P}_1^{(4)}$  is a *two-parameter* family and may contain direct and indirect product bases. Notice that the operator  $\hat{s}_\mu$  can act as the identity since the first basis of  $\mathcal{P}_1^{(4)}$  may be the standard basis  $\{|j_z, k_z\rangle\}$ .

The pair  $\mathcal{P}_1^{(4)}$  turns out to be *equivalent* under *non-local* transformations to the Fourier basis as follows from mapping the first basis to the standard basis  $\{|j_z, k_z\rangle\}$ . Thus, we have obtained all known pairs of MU bases in dimension four (cf. Sec. 3 of [14]) in spite of limiting ourselves initially to MU product bases only.

### 5.2 All triples of MU product bases

Now we are in a position to derive all triples of MU product bases in dimension  $d = 4$ : we need to determine which of the pairs of MU product bases given in Proposition 1 can be extended by a third MU product basis.

It is easy to see that the MU pair  $\mathcal{P}_0^{(4)} \equiv \{|j_z, k_z\rangle; |j_x, k_x\rangle\}$  can be extended by adjoining a third direct product basis, namely  $|j_y, k_y\rangle$ , resulting in the standard Heisenberg-Weyl triple. This is the *only* possibility, as follows immediately from

Theorem 1: a product state  $|\phi, \Phi\rangle$  is MU to both  $\{|j_z, k_z\rangle\}$  and  $\{|j_x, k_x\rangle\}$  only if  $|\phi\rangle$  is MU both to  $\{|j_z\rangle\}$  and  $\{|j_x\rangle\}$ , and if  $|\Phi\rangle$  is MU both to  $\{|k_z\rangle\}$  and  $\{|k_x\rangle\}$ .

The pair  $\mathcal{P}_1^{(4)}$  of MU bases cannot be extended, not even by a single MU product state. To extend the pair by an MU product state, one would need to find a state in  $\mathbb{C}^2$  which is MU to the three bases  $\{|k_z\rangle\}$ ,  $\{|k_x\rangle\}$  and  $\{|\hat{r}_\nu k_x\rangle\}$ . Since  $\nu \in (0, \pi)$ , no two of these three bases coincide and there is no state in the space  $\mathbb{C}^2$  simultaneously MU to three distinct bases. As a consequence, the number of MU product triples is rather limited in dimension four.

**Proposition 2.** *Any triple of MU product bases in the space  $\mathbb{C}^2 \otimes \mathbb{C}^2$  is equivalent to*

$$\mathcal{T}_0^{(4)} \equiv \{|j_z, k_z\rangle; |j_x, k_x\rangle; |j_y, k_y\rangle\} . \quad (32)$$

Using Theorem 1 again, the non-existence of even a single product state MU to the triple  $\mathcal{T}_0^{(4)}$  follows immediately—all states MU to the triple must be entangled.

This observation agrees with results reported earlier. For the two-qubit system considered here, a construction of the five MU bases based on the Galois field  $GF(4)$  has been given in [18]. The complete sets obtained turn out to be equivalent under local unitary transformations, and they necessarily consist of three MU bases made up from separable (i.e. product) bases while the remaining two contain maximally entangled states only. This structure also emerges from an approach which exploits the fact that any *complete* set of MU bases of a bipartite system in  $\mathbb{C}^d$  contains a *fixed*  $d$ -dependent amount of entanglement [10]. When  $d = 4$ , this result implies that for a complete set of MU bases containing the triple  $\mathcal{T}_0^{(4)}$ , the other two bases of the quintuple must consist of *entangled* states – in fact, only maximally entangled states are permitted. In [11], the entanglement structure of complete sets of MU bases related to Heisenberg-Weyl operators in prime-power dimensions has been studied leading to a generalization of the result for dimension  $d = 4$ : in bipartite systems of dimension  $d = p^2$  a number of  $(p + 1)$  MU bases must consist of product states while the remaining ones contain only maximally entangled states.

## 6 MU product bases in dimension six

### 6.1 All pairs of MU product bases

We will now construct all pairs of MU product bases in dimension six following the method used in dimension four (cf. Sec. 3.1). To obtain a MU pair we take each



basis listed in Lemma 2 and go through all possibilities of adding one of the product bases  $\mathcal{B}_0$  to  $\mathcal{B}_3$  (cf. Eqs. (47,46,50,51) of Appendix A).

When constructing pairs of MU product bases, it is not necessary to include the basis  $\mathcal{I}_2$  in Lemma 2. We will show now that the operator  $\hat{V}$  must either act as the identity on the pair of states  $\{|1_z\rangle, |2_z\rangle\}$  or swap them, i.e. only  $\alpha = 0$  or  $\beta = 0$  are allowed in the expression  $\hat{V}|1_z\rangle = \alpha|1_z\rangle + \beta|2_z\rangle$ . However, in both cases the simplified product basis  $\mathcal{I}_2$  turns into a special case of  $\mathcal{I}_3$ , given in (28).

Here is the reason why the operator  $\hat{V}$  must simplify in the way just described. Apply Theorem 1 to the product state  $|\phi, \Phi\rangle$  required to be MU to  $\mathcal{I}_2$ : the state  $|\Phi\rangle$  must be MU to all six vectors of  $\mathbb{C}^3$  present in  $\mathcal{I}_2$ . Consequently, all states in  $\mathbb{C}^3$  which occur in the bases  $\mathcal{B}_0$  to  $\mathcal{B}_3$ , defined in Eqs. (47,46,50,51) – these are all candidates for a second product basis MU to  $\mathcal{I}_2$  – must be MU to the standard basis  $\{|J_z\rangle\}$  of  $\mathbb{C}^3$ . Now, each of these four bases contains another orthonormal basis of  $\mathbb{C}^3$ , namely  $\{|A\rangle, |A^\perp\rangle, |A^\perp\rangle\}$ . There is a two-parameter family of such states, given in Eq. (15). However, these states must also be MU to the state  $\hat{V}|1_z\rangle$  of the basis  $\mathcal{I}_2$ . For the states  $|A\rangle$  and  $|A^\perp\rangle$ , this requirement reads

$$|\langle A | (\alpha|1_z\rangle + \beta|2_z\rangle) \rangle|^2 = |\langle A^\perp | (\alpha|1_z\rangle + \beta|2_z\rangle) \rangle|^2 = \frac{1}{3}. \quad (33)$$

Now using the explicit expressions of the states  $|A\rangle$  and  $|A^\perp\rangle$  given in Eq. (16) and the identity  $|\alpha|^2 + |\beta|^2 = 1$ , the first equality leads to

$$|1 + \omega| |\alpha| |\beta| = |\alpha| |\beta|, \quad (34)$$

which implies that either  $\alpha \equiv 0$  or  $\beta \equiv 0$ . Thus, for the construction of pairs it is sufficient to use the restricted basis

$$\mathcal{I}'_2 = \{|j_z, 0_z\rangle, |\hat{u}j_z, 1_z\rangle, |\hat{u}j_z, 2_z\rangle\} \quad (35)$$

instead of  $\mathcal{I}_2$  given in Lemma 2. All bases of this form, however, are contained in  $\mathcal{I}_3$  if one chooses  $\hat{v} = \hat{w} \equiv \hat{u}$  in (28). This simplification also holds for the basis  $\mathcal{B}_2$  when occurring in a pair of product bases.

The actual derivation of all MU product bases in dimension six is lengthy but straightforward. The calculations have been relegated to Appendix B except for the pairing of the basis  $\mathcal{I}_1$  with  $\mathcal{B}_1$ , which gives rise to the pair  $\mathcal{P}_3$ . The proof that no other (non-trivial) pair of MU product bases results from  $\{\mathcal{I}_1; \mathcal{B}_1\}$  has been obtained by A. Sudbery, and it is given in Appendix C. We now summarise the results derived in these two appendices.

**Theorem 2.** Any pair of MU product bases in the space  $\mathbb{C}^2 \otimes \mathbb{C}^3$  is equivalent to a member of the families

$$\begin{aligned}\mathcal{P}_0 &= \{|j_z, J_z\rangle; |j_x, J_x\rangle\}, \\ \mathcal{P}_1 &= \{|j_z, J_z\rangle; |0_x, J_x\rangle, |1_x, \hat{R}_{\xi, \eta} J_x\rangle\}, \\ \mathcal{P}_2 &= \{|0_z, J_z\rangle, |1_z, J_y\rangle; |0_x, J_x\rangle, |1_x, J_w\rangle\}, \\ \mathcal{P}_3 &= \{|0_z, J_z\rangle, |1_z, \hat{S}_{\zeta, \chi} J_z\rangle; |j_x, 0_x\rangle, |\hat{r}_\sigma j_x, 1_x\rangle, |\hat{r}_\tau j_x, 2_x\rangle\},\end{aligned}\tag{36}$$

with  $j = 0, 1$  and  $J = 0, 1, 2$ . The unitary operator  $\hat{R}_{\xi, \eta}$  is defined as  $\hat{R}_{\xi, \eta} = |0_z\rangle\langle 0_z| + e^{i\xi}|1_z\rangle\langle 1_z| + e^{i\eta}|2_z\rangle\langle 2_z|$ , for  $\eta, \xi \in [0, 2\pi)$ , and  $\hat{S}_{\zeta, \chi}$  is defined analogously with respect to the  $x$ -basis; the unitary operators  $\hat{r}_\sigma$  and  $\hat{r}_\tau$  act on the basis  $\{|j_x\rangle\} \equiv \{|\pm\rangle\}$  according to  $\hat{r}_\sigma|j_x\rangle = (|0_z\rangle \pm e^{i\sigma}|1_z\rangle)/\sqrt{2}$  for  $\sigma \in (0, \pi)$ , etc.

As before, the ranges of the parameters are assumed to be such that no MU product pair occurs more than once in the list. The pairs  $\mathcal{P}_0$  and  $\mathcal{P}_2$  have no parameter dependence, the pair  $\mathcal{P}_1$  depends on two parameters, while  $\mathcal{P}_3$  is a four-parameter family.

Theorem 2 represents the first main result of this paper. It states that there are continuously many possibilities to select pairs of MU bases which, however, can be listed exhaustively. In the remainder of this paper we will proceed by *analytically* constructing all *triples* of MU bases which exist in  $d = 6$ . This will lead to our most important result, namely Theorem 4 in Sec. 7 which states the impossibility to extend any MU product triple by even a single MU vector. Thus, complete sets of MU bases in  $d = 6$  will contain at most *pairs* of MU product bases.

An alternative method to exploit Theorem 2 has been pursued in [20]. Upon using suitable *non-local* unitary transformations and known results obtained by computer-algebraic methods, the strongest possible statement about MU product bases is then derived: if a complete set of seven MU bases exists, it will contain at most *one* product basis – which may be chosen to be the standard basis.

## 6.2 All triples of MU product bases

It is straightforward to enlarge the existing pairs of MU product bases in Theorem 2 to triples: simply add the MU product bases listed in Lemma 2, one after the other, to each of the pairs  $\mathcal{P}_0$  to  $\mathcal{P}_3$  and check whether a valid MU product triple results.

Neither of the pairs  $\mathcal{P}_2$  and  $\mathcal{P}_3$  in Theorem 2 can be extended by a single MU product state. To do so, we would need a vector MU to the three distinct bases  $\{|j_z\rangle\}$ ,  $\{|j_x\rangle\}$

and  $\{|\hat{r}_\sigma j_x\rangle\}$  in the space  $\mathbb{C}^2$ , or a vector mutually unbiased to four MU bases in the space  $\mathbb{C}^3$ . No such states exist, implying that any state mutually unbiased to these pairs must be entangled.

The pairs  $\mathcal{P}_0$  and  $\mathcal{P}_1$  can be extended by a further MU product basis since there exist vectors of the spaces  $\mathbb{C}^2$  and  $\mathbb{C}^3$  that satisfy the necessary conditions. To obtain the complete list of all MU product triples in  $\mathbb{C}^6$  we thus need to search for possible extensions of these two pairs by a third product basis. Starting with  $\mathcal{P}_0$ , it is possible to extend this pair by either  $\mathcal{B}_0$  or  $\mathcal{B}_1$ .

- $\{\mathcal{P}_0; \mathcal{B}_0\}$ : If we choose the third basis to be of the form  $\mathcal{B}_0$ , there are only two choices,  $\{|j_y, J_y\rangle\}$  or  $\{|j_y, J_w\rangle\}$ . Using the local complex conjugation  $\hat{I} \otimes \hat{K}$ , the resulting triples are found to be equivalent,

$$\{|j_z, J_z\rangle; |j_x, J_x\rangle; |j_y, J_y\rangle\} \sim \{|j_z, J_z\rangle; |j_x, J_x\rangle; |j_y, J_w\rangle\}; \quad (37)$$

consequently, all triples of this type are equivalent to the Heisenberg-Weyl triple

$$\mathcal{T}_0 = \{|j_z, J_z\rangle; |j_x, J_x\rangle; |j_y, J_y\rangle\}. \quad (38)$$

- $\{\mathcal{P}_0; \mathcal{B}_1\}$ : If we extend  $\mathcal{P}_0$  by an indirect product basis of the form  $\mathcal{B}_1$ , there are only two choices,  $\{|0_y, J_y\rangle, |1_y, J_w\rangle\}$  or  $\{|0_y, J_w\rangle, |1_y, J_y\rangle\}$ . Again, a local complex conjugation  $\hat{k} \otimes \hat{I}$  maps one of the triples into the other,

$$\{|j_z, J_z\rangle; |j_x, J_x\rangle; |0_y, J_y\rangle, |1_y, J_w\rangle\} \sim \{|j_z, J_z\rangle; |j_x, J_x\rangle; |0_y, J_w\rangle, |1_y, J_y\rangle\}, \quad (39)$$

leaving us with the triple

$$\mathcal{T}_1 = \{|j_z, J_z\rangle; |j_x, J_x\rangle; |0_y, J_y\rangle, |1_y, J_w\rangle\}. \quad (40)$$

Now turning to the pair  $\mathcal{P}_1$ , we again attempt to obtain a triple by adding either  $\mathcal{B}_0$  or  $\mathcal{B}_1$ .

- $\{\mathcal{P}_1; \mathcal{B}_0\}$  or  $\{\mathcal{P}_1; \mathcal{B}_1\}$ : First, extend the pair  $\mathcal{P}_1$  by a direct product basis, resulting in either  $\{|j_z, J_z\rangle; |0_x, J_x\rangle, |1_x, J_y\rangle; |j_y, J_w\rangle\}$  or  $\{|j_z, J_z\rangle; |0_x, J_x\rangle, |1_x, J_w\rangle; |j_y, J_y\rangle\}$ . It is not difficult to apply suitable LETs to transform them into the triple  $\mathcal{T}_1$ . Now extend the pair  $\mathcal{P}_1$  by an indirect product basis  $\mathcal{B}_1$ . This leads to a contradiction since we would need the states  $\{|\hat{R}_{\xi, \eta} J_x\rangle\}$  in  $\mathcal{P}_1$  to coincide with  $\{|J_x\rangle\}$ , which is not allowed.

This completes the construction of all MU product triples in dimension six, leading to the second main result of this paper.

**Theorem 3.** *Any triple of MU product bases in the space  $\mathbb{C}^2 \otimes \mathbb{C}^3$  is equivalent to either*

$$\begin{aligned} \mathcal{T}_0 &= \{|j_z, J_z\rangle; |j_x, J_x\rangle; |j_y, J_y\rangle\}, \\ \text{or } \mathcal{T}_1 &= \{|j_z, J_z\rangle; |j_x, J_x\rangle; |0_y, J_y\rangle, |1_y, J_w\rangle\}. \end{aligned} \quad (41)$$

According to Theorem 1, neither of these triples can be extended by a single MU product state. Thus, any complete set of seven MU bases in dimension six will contain at most three product bases, and if it does, the triple must be equivalent to one of those in Theorem 3. In the following section we will obtain an even stronger result.

## 7 Excluding triples of MU product bases from complete sets

In this section we derive the third main result of this paper.

**Theorem 4.** *No triple of MU product bases in dimension six can be extended by a single MU vector.*

In other words, no complete set of seven MU bases in  $d = 6$  contains a triple of MU product bases. This result relies on a computer-algebraic proof in [6], which finds a total of 48 vectors MU to the pair of eigenbases of the Heisenberg-Weyl operators  $X_6$  and  $Z_6$ , giving rise to sixteen different orthonormal bases. However, none of these bases allows one to extend the given pair beyond a triple of MU bases.

The present construction of MU product triples effectively produces twelve (and only twelve) product vectors that are MU to the pair  $\mathcal{P}_0 = \{|j_z, J_z\rangle; |j_x, J_x\rangle\}$ , namely  $\{|j_y, J_y\rangle\}$  and  $\{|j_y, J_w\rangle\}$ , and they give rise to the only two inequivalent triples of MU bases,  $\mathcal{T}_0$  and  $\mathcal{T}_1$ . Since  $\mathcal{P}_0$  is equivalent to the eigenbases of  $X_6$  and  $Z_6$ , clearly these twelve product vectors must figure among the 48 vectors given in [6].

To show this, we must first deal with a difference in our definition of the HW operators. The HW pair used in [6] does not have the same form as  $\mathcal{P}_0$  since the  $x$ -basis in [6] is the eigenbasis of the operator  $X_6$ , whereas we have used the eigenbasis of the operator  $X_2 \otimes X_3$  (cf. Eq. (5)). Nevertheless, both pairs of bases turn out to be equivalent using a *non-local* unitary transformation. By writing the operators as matrices, we find that  $X_2 \otimes X_3 = P_{25} X_6 P_{25}$ , where  $P_{25}$  is a permutation matrix

permuting rows two and five. This non-local transformation brings the eigenbasis of  $X_6$  into product form, i.e.  $\{|j_x, J_x\rangle\}$ , by multiplying it with  $P_{25}$  from the left.

The same transformation must also be applied to the list of 48 vectors so that they are MU to the pair  $\mathcal{P}_0$ . After multiplying each of these vectors by the matrix  $P_{25}$  from the left, one easily identifies the twelve product vectors, numbered by 1, 2, 5, 6, 9, 10, 13, 14, 17, 18, 21 and 22 in the Appendix of the updated version of [6]. For example, the vector labelled (1) transforms as follows:

$$\begin{aligned} \frac{1}{\sqrt{6}} P_{25} (1, \alpha^5, 1, -\alpha^3, -\alpha^2, -\alpha^3)^T &= \frac{1}{\sqrt{6}} (1, -\alpha^2, 1, -\alpha^3, \alpha^5, -\alpha^3)^T \\ &\equiv \frac{1}{\sqrt{6}} (1, \omega^2, 1, -i, -i\omega^2, -i)^T \\ &\equiv \frac{1}{\sqrt{6}} (1, -i)^T \otimes (1, \omega^2, 1)^T \end{aligned} \quad (42)$$

where  $\alpha = e^{2\pi i/12}$  and  $\omega = e^{2\pi i/3}$ . This vector is the product state  $|1_y, 1_y\rangle$ .

The twelve vectors give rise to four of the sixteen orthonormal bases which are MU to the original pair. These product bases are covered by the product bases we construct when extending the Heisenberg-Weyl pair  $\mathcal{P}_0$  to a triple; however, only two of the four triples are locally inequivalent as follows from exploiting suitable local equivalence transformations.

Upon combining the computer-aided result just described with Theorem 3 it is straightforward to arrive at a result that excludes product triples from being part of a complete set of seven MU bases. The triples of MU product bases  $\mathcal{T}_0$  and  $\mathcal{T}_1$  both contain the Heisenberg-Weyl pair  $\mathcal{P}_0 = \{|j_z, J_z\rangle; |j_x, J_x\rangle\}$ , and it is impossible to extend this pair by more than a single MU basis according to [6]. Since Theorem 3 provides an *exhaustive* list of MU triples in the space  $\mathbb{C}^2 \otimes \mathbb{C}^3$ , it follows that *no complete set of seven MU bases in  $d = 6$  contains a triple of MU product bases*.

## 8 Summary and discussion

By limiting ourselves to orthonormal product bases, we have been able to obtain a number of analytic results regarding the existence of MU bases of the space  $\mathbb{C}^2 \otimes \mathbb{C}^3$ . After identifying all orthonormal product bases of this space, presented in Lemma 2, we have constructed an exhaustive list of pairs of MU product bases. They come in four different flavours according to Theorem 2. Next, Theorem 3 states that, in addition to the Heisenberg-Weyl triple, there is only one other locally

inequivalent triple of MU product bases. The absence of quadruples of MU product bases agrees with Zauner’s conjecture [19] that there are no more than three MU bases in dimension six.

The derivation of the list of MU product pairs and triples has been simplified considerably by the content of Theorem 1. It spells out severe restrictions on the form of product states required to be MU to certain sets of orthonormal states in the space  $\mathbb{C}^2 \otimes \mathbb{C}^3$ . We have established Theorem 1 for dimensions  $d = 4$  and  $d = 6$  only, since the proof relies on enumerating all orthonormal product bases in these dimensions.

Theorem 3 allows us to partly replicate results obtained by means of a computer-algebraic method. Out of the 48 vectors mutually unbiased to the Heisenberg-Weyl pair  $\mathcal{P}_0$ , found in [6], we successfully recover twelve, and they are shown to be equivalent to product vectors.

The most important consequence of exhaustively enumerating MU product bases in dimension six is a bound on their allowed number in complete sets of MU bases. Applying Theorem 1 to the triples of MU product bases in  $\mathbb{C}^2 \otimes \mathbb{C}^3$ , namely  $\mathcal{T}_0$  and  $\mathcal{T}_1$ , directly implies that no single *product* state can be MU to any of them. However, a stronger result is within reach, spelled out in Theorem 4: it is impossible to complement either  $\mathcal{T}_0$  or  $\mathcal{T}_1$  by *any* MU vector. This follows from combining Theorem 3 with the results derived in [6]. Thus, *a complete set of MU bases in dimension six cannot contain a product triple*. This is in marked contrast to the prime-power dimension  $p^2$  where a complete set of MU bases necessarily contains  $(p+1)$  MU product bases constructed from the tensor products of Heisenberg-Weyl operators [11]. The exhaustive list of MU product pairs given in Theorem 2 has been used to derive a result even stronger than Theorem 4, reducing the number of allowed MU product bases to just a single one [20].

A similar situation has been described in [21] where a different class of MU bases is studied. Given a “nice unitary error basis”, consisting of  $d^2$  suitable matrices, one can search for MU bases within these sets. In the case of dimension six, it is shown that any partition of a nice error basis gives rise to no more than three MU bases. This limitation and the non-existence of more than three MU *product* bases are independent results: MU product bases and MU bases arising from nice unitary error bases are structurally different. For example, our construction reproduces the continuous family  $\mathcal{P}_1^{(4)}$  of MU product pairs in  $d = 4$ , and it is known that some of the pairs in this family are *inequivalent* to MU bases stemming from nice unitary error bases [22].

Our considerations are backed by deriving corresponding results in the Hilbert space

of two qubits, i.e.  $\mathbb{C}^2 \otimes \mathbb{C}^2$ . In this case there exists a symmetry between the two factors and the enumeration of MU product pairs and triples is much simpler. Clearly, when a qubit is combined with a qutrit, no such symmetry exists. We believe that the symmetries between the subsystems present in only prime-power dimensions are the ultimate reason that additional “identities” exist which allow for the construction of *complete* sets of MU bases.

Let us conclude by formulating a conjecture which emerges naturally from our results: we expect Theorem 1 to hold for *all* composite dimensions  $d = pq \geq 4$ , not only for  $d = 4$  and  $d = 6$ . Our pedestrian proof in these dimensions relies on enumerating all orthonormal product bases. However, the set of product bases in composite dimensions is likely to possess a certain structure which, once spelled out, should allow for a more elegant proof applicable to arbitrary composite dimensions.

## Acknowledgements

The proof of Theorem 5, presented in Appendix C, has been found by A. Sudbery; we gratefully acknowledge his permission to reproduce it here. We thank S. Brierley, M. Grassl, and A. Sudbery for comments and suggestions. This work has been supported by EPSRC.

## References

- [1] I. D. Ivanović, *J. Phys. A* **14**, 3241 (1981).
- [2] W. K. Wootters and B. D. Fields, *Ann. Phys. (N.Y.)* **191**, 363 (1989).
- [3] T. Durt, B-G. Englert, I. Bengtsson and K. Życzkowski, *Int. J. Quant. Inf.* **8**, 535 (2010).
- [4] P. Butterley and W. Hall, *Phys. Lett. A* **369**, 5 (2007).
- [5] S. Brierley and S. Weigert, *Phys. Rev. A* **78**, 042312 (2008).
- [6] M. Grassl, in *Proc. ERATO Conf. on Quantum Information Science 2004 (EQIS 2004)*; also: e-print arXiv:quant-ph/0406175 (2004).
- [7] S. Brierley and S. Weigert, *Phys. Rev. A* **79**, 052316 (2009).
- [8] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi and M. Weiner, *J. Phys. A: Math. Theor.* **42**, 245305 (2009).

- [9] J. L. Romero, G. Björk, A. B. Klimov, and L. L. Sánchez-Soto, *Phys. Rev. A* **72**, 062310 (2005).
- [10] M. Wieśniak, T. Paterek and A. Zeilinger, *New J. Phys.* **13**, 053047 (2011).
- [11] J. Lawrence, *Phys. Rev. A* **84**, 022338 (2011).
- [12] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan, *Algorithmica*, **34**, 512 (2002).
- [13] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin and W. K. Wootters, *Phys. Rev. A* **59**, 1070 (1999).
- [14] S. Brierley, S. Weigert and I. Bengtsson, *Quantum. Inf. Comput.* **10**, 803 (2010).
- [15] I. Bengtsson, W. Bruzda, Å. Ericsson, J-Å. Larsson, W. Tadej and K. Życzkowski, *J. Math. Phys.* **48**, 052106 (2007).
- [16] M. A. Nielsen, *Phys. Rev. Lett.* **83**, 436 (1999).
- [17] E. P. Wigner, *Gruppentheorie und ihre Anwendung auf die Quantenmechanik der Atomspektren*, (Braunschweig, 1931).
- [18] A. B. Klimov, J. L. Romero, G. Björk and L. L. Sánchez-Soto, *J. Phys. A* **40**, 3987 (2007).
- [19] G. Zauner, *Int. J. Quantum. Inf.* **9**, 445 (2011).
- [20] D. McNulty and S. Weigert, *J. Phys. A: Math. Theor.* **45**, 102001 (2012).
- [21] M. Aschbacher, A. M. Childs, and P. Wocjan, *J. Algebr. Comb.* **25**, 111 (2007).
- [22] A. Klappenecker and M. Rötteler, *IEEE Trans. Inform. Theory*, **51** (2005)

## A Appendix

In this Appendix we derive all product bases in dimension six reported in Lemma 2. The six states  $|\psi_j\rangle, j = 1 \dots 6$ , of a product basis  $\{|\psi_j, \Psi_j\rangle\}$ , defined in (26) must contain at least *two* (possibly identical) pairs of orthogonal states. If there was only one pair (with the remaining four states of the space  $\mathbb{C}^2$  non-orthogonal), the orthogonality conditions (27) would require *four* orthogonal states  $|\Psi_j\rangle \in \mathbb{C}^3$ , which



do not exist. Thus, denoting the orthogonal pairs by  $\{|a\rangle, |a^\perp\rangle\}$  and  $\{|b\rangle, |b^\perp\rangle\}$ , the product basis must take the form

$$\left\{ |a, \Psi_1\rangle, |a^\perp, \Psi_2\rangle, |b, \Psi_3\rangle, |b^\perp, \Psi_4\rangle, |\psi_5, \Psi_5\rangle, |\psi_6, \Psi_6\rangle \right\}. \quad (43)$$

The states  $|\psi_5\rangle$  and  $|\psi_6\rangle$  must also be an orthogonal pair. To see this, assume that they are skew (or identical) *and* they are both skew to the states  $|a\rangle$  and  $|b\rangle$ ; then the state  $|\Psi_6\rangle$ , for example, must be orthogonal to the orthonormal triple  $\{|\Psi_1\rangle, |\Psi_3\rangle, |\Psi_5\rangle\}$ , which is impossible. Here we have assumed that  $|a\rangle$  and  $|b\rangle$  are *not* orthogonal; if they are, we use the orthonormal triple  $\{|\Psi_1\rangle, |\Psi_4\rangle, |\Psi_5\rangle\}$  instead. The same conclusion can be drawn if the states  $|\psi_5\rangle$  and  $|\psi_6\rangle$  are skew (or identical) but one of them coincides with any of the four states  $|a\rangle, |b\rangle, |a^\perp\rangle$  or  $|b^\perp\rangle$ . Thus, we conclude that any product basis of the space  $\mathbb{C}^6$  must be of the form

$$\left\{ |a, \Psi_1\rangle, |a^\perp, \Psi_2\rangle, |b, \Psi_3\rangle, |b^\perp, \Psi_4\rangle, |c, \Psi_5\rangle, |c^\perp, \Psi_6\rangle \right\}. \quad (44)$$

Now it is obvious that we need to consider three different possibilities depending on how many of the three bases of the space  $\mathbb{C}^2$  coincide.

**Case 1:** If all three bases coincide, we have

$$\left\{ |a, \Psi_1\rangle, |a^\perp, \Psi_2\rangle, |a, \Psi_3\rangle, |a^\perp, \Psi_4\rangle, |a, \Psi_5\rangle, |a^\perp, \Psi_6\rangle \right\}. \quad (45)$$

These six states are orthogonal only if the three states  $|\Psi_1\rangle, |\Psi_3\rangle$  and  $|\Psi_5\rangle$  are orthogonal to each other, as well as the triple  $\{|\Psi_2\rangle, |\Psi_4\rangle, |\Psi_6\rangle\}$ . Upon denoting the first triple by  $\{|A\rangle, |A^\perp\rangle, |A^\perp\rangle\}$ , where  $|A^\perp\rangle \in \mathbb{C}^3$  is a vector orthogonal to  $|A\rangle$  and  $|A^\perp\rangle$ , we obtain

$$\mathcal{B}_1 = \left\{ |a, A\rangle, |a, A^\perp\rangle, |a, A^\perp\rangle, |a^\perp, A\rangle, |a^\perp, A^\perp\rangle, |a^\perp, A^\perp\rangle \right\}, \quad (46)$$

also introducing an arbitrary second triple of orthogonal states. If the two triples coincide, we find the important special case of a direct product basis

$$\mathcal{B}_0 = \left\{ |a, A\rangle, |a, A^\perp\rangle, |a, A^\perp\rangle, |a^\perp, A\rangle, |a^\perp, A^\perp\rangle, |a^\perp, A^\perp\rangle \right\}, \quad (47)$$

**Case 2:** If only two of the bases in  $\mathbb{C}^2$  coincide, we find

$$\left\{ |a, \Psi_1\rangle, |a^\perp, \Psi_2\rangle, |b, \Psi_3\rangle, |b^\perp, \Psi_4\rangle, |b, \Psi_5\rangle, |b^\perp, \Psi_6\rangle \right\}. \quad (48)$$

As in Case 1, each of the triples  $\{|\Psi_1\rangle, |\Psi_3\rangle, |\Psi_5\rangle\}$  and  $\{|\Psi_2\rangle, |\Psi_4\rangle, |\Psi_6\rangle\}$  must be an orthonormal basis of  $\mathbb{C}^3$ . However, we also need to have

$$\langle \Psi_1 | \Psi_4 \rangle = \langle \Psi_1 | \Psi_6 \rangle = 0, \quad (49)$$

which means that  $|\Psi_3\rangle$  and  $|\Psi_5\rangle$  span the same subspace as  $|\Psi_4\rangle$  and  $|\Psi_6\rangle$ . It follows that  $|\Psi_1\rangle \equiv |\Psi_2\rangle$ ; upon calling this state  $|A\rangle$ , we are led to a new class of product bases of  $\mathbb{C}^6$  given by

$$\mathcal{B}_2 = \left\{ |a, A\rangle, |a^\perp, A\rangle, |b, A^\perp\rangle, |b^\perp, \hat{V}A^\perp\rangle, |b, A^\perp\rangle, |b^\perp, \hat{V}A^\perp\rangle \right\}, \quad (50)$$

where  $\hat{V}|A^\perp\rangle = \alpha|A^\perp\rangle + \beta|A^\perp\rangle$  and  $\hat{V}|A^\perp\rangle = \bar{\beta}|A^\perp\rangle - \bar{\alpha}|A^\perp\rangle$ , i.e.  $\hat{V}$  is any unitary transformation of the two-dimensional subspace of  $\mathbb{C}^3$  orthogonal to the state  $|A\rangle$ .

**Case 3:** Finally, we consider the case where the three bases of the space  $\mathbb{C}^2$  present in (44) are all different, meaning that  $|a\rangle$ ,  $|b\rangle$ , and  $|c\rangle$  are pairwise skew. Then, the orthogonality conditions directly imply that the triples  $\{|\Psi_1\rangle, |\Psi_3\rangle, |\Psi_5\rangle\}$  and  $\{|\Psi_2\rangle, |\Psi_4\rangle, |\Psi_6\rangle\}$  of orthogonal states must coincide. This leaves us with bases of the form

$$\mathcal{B}_3 = \left\{ |a, A\rangle, |a^\perp, A\rangle, |b, A^\perp\rangle, |b^\perp, A^\perp\rangle, |c, A^\perp\rangle, |c^\perp, A^\perp\rangle \right\}. \quad (51)$$

These three cases complete the construction of all product bases in dimension six. Using local equivalence transformations in analogy to the procedure used in Sec. 3.1, one can write the four sets of product bases as displayed in Lemma 2.

## B Appendix

In this Appendix we derive all pairs of MU product bases in dimension six by pairwise combining the orthonormal product bases  $\mathcal{B}_0$  to  $\mathcal{B}_3$ , defined in Eqs. (47,46,50,51). In principle, we need to look at only 10 of the 16 pairs  $\{\mathcal{B}_i; \mathcal{B}_j\}$ ,  $i, j = 0 \dots 3$ , since the order of the bases does not matter: the pairs  $\{\mathcal{B}_i; \mathcal{B}_j\}$  and  $\{\mathcal{B}_j; \mathcal{B}_i\}$  are equivalent for  $i \neq j$ . Using local equivalence transformations, each pair can be brought to the form  $\{\mathcal{I}_i; \mathcal{B}_j\}$ ,  $i \leq j$ , where the bases  $\mathcal{I}_0$  to  $\mathcal{I}_3$  are those listed in Lemma 2. As shown in the main text, it is not actually necessary to consider the bases  $\mathcal{I}_2$  and  $\mathcal{B}_2$  at all, reducing the number of cases to six. Parameter ranges are assumed so that no pair occurs more than once.

- $\{\mathcal{I}_0; \mathcal{B}_0\}$ : First we extend  $\mathcal{I}_0$  to a pair of MU bases by combining it with

$$\mathcal{B}_0 = \left\{ |a, A\rangle, |a, A^\perp\rangle, |a, A^\perp\rangle, |a^\perp, A\rangle, |a^\perp, A^\perp\rangle, |a^\perp, A^\perp\rangle \right\}. \quad (52)$$

The states of  $\mathcal{B}_0$  are MU to those of the basis  $\mathcal{I}_0$  if the pair of states  $\{|a\rangle, |a^\perp\rangle\}$  is any basis of  $\mathbb{C}^2$  associated with opposite points on the Bloch sphere, i.e.  $|a\rangle =$

$(|0_z\rangle + e^{i\mu}|1_z\rangle)/\sqrt{2}$  etc., and if the orthonormal basis  $\{|A\rangle, |A^\perp\rangle, |A^\perp\rangle\}$  is defined as in Eqs. (15) of Sec. 2.2.

A local transformation allows us to rotate the states  $\{|a\rangle, |a^\perp\rangle\}$  into  $\{|j_x\rangle\}$  and to simultaneously change the basis  $\{|A\rangle, |A^\perp\rangle, |A^\perp\rangle\}$  into the basis  $\{|J_x\rangle\}$  of  $\mathbb{C}^3$  so that we end up with the known Heisenberg-Weyl MU pair of direct product bases,

$$\mathcal{P}_0 \equiv \{|j_z, J_z\rangle; |j_x, J_x\rangle\}. \quad (53)$$

•  $\{\mathcal{I}_0; \mathcal{B}_1\}$  and  $\{\mathcal{I}_0; \mathcal{B}_3\}$ : These cases will be covered by the pairs  $\{\mathcal{I}_1; \mathcal{B}_1\}$  and  $\{\mathcal{I}_1; \mathcal{B}_3\}$ , respectively, since we can treat the basis  $\mathcal{I}_0$  as a subset of  $\mathcal{I}_1$ .

We now construct the three pairs of indirect product bases that contain  $\mathcal{I}_1 = \{|0_z, J_z\rangle, |1_z, \hat{U}J_z\rangle\}$  as the first basis, where the unitary  $\hat{U}$  maps the basis  $\{|J_z\rangle\}$  of the space  $\mathbb{C}^3$  to another basis.

•  $\{\mathcal{I}_1; \mathcal{B}_1\}$ : In a first step, we act with a local unitary on the second basis

$$\mathcal{B}_1 = \left\{ |a, A\rangle, |a, A^\perp\rangle, |a, A^\perp\rangle, |a^\perp, B\rangle, |a^\perp, B^\perp\rangle, |a^\perp, B^\perp\rangle \right\} \quad (54)$$

to rotate the  $a$ -basis of states that are MU to  $\{|j_z\rangle\}$  into the basis  $\{|j_x\rangle\}$  while the  $A$ -basis turns into  $\{|J_x\rangle\}$ , as before. This maps  $\mathcal{B}_1$  to

$$\left\{ |0_x, J_x\rangle, |1_x, \hat{U}'J_x\rangle \right\}, \quad (55)$$

where we have introduced a unitary  $\hat{U}'$  which parameterises all orthonormal bases of  $\mathbb{C}^3$  relative to the  $x$ -basis. The requirement that the states of the pair  $\{\mathcal{I}_1; \mathcal{B}_1\}$  be MU now turns into the problem of identifying all pairs of orthonormal bases of  $\mathbb{C}^3$ , namely  $\{|J_z\rangle; |\hat{U}J_z\rangle\}$  and  $\{|J_x\rangle; |\hat{U}'J_x\rangle\}$ , such that all states of one set are MU to those of the other, viz.

$$|\langle J_z | \hat{U}'J_x \rangle|^2 = |\langle \hat{U}J_z | J_x \rangle|^2 = |\langle \hat{U}J_z | \hat{U}'J_x \rangle|^2 = \frac{1}{3}, \quad (56)$$

while  $|\langle J_z | J_x \rangle|^2 = 1/3$  holds by construction. It is easy to see that these conditions are satisfied if the bases in (at least) one pair coincide or all four are different, i.e. they use up a complete set of MU bases in  $\mathbb{C}^3$ . In Appendix C we present a proof, due to A. Sudbery, that these are the *only* solutions of the constraints (56). Thus, if  $\mathcal{I}_1$  is the standard basis  $\{|j_z, J_z\rangle\}$ , then we obtain the MU product pair

$$\mathcal{P}_1 = \{|j_z, J_z\rangle; |0_x, J_x\rangle, |1_x, \hat{R}_{\xi, \eta}J_x\rangle\}, \quad (57)$$

with  $\{|\hat{R}_{\xi, \eta}J_x\rangle\}$  defined in Eq. (15). However, if we use the complete set of MU bases in  $\mathbb{C}^3$  we obtain the MU product pair

$$\mathcal{P}_2 = \{|0_z, J_z\rangle, |1_z, J_y\rangle; |0_x, J_x\rangle, |1_x, J_w\rangle\}. \quad (58)$$

- $\{\mathcal{I}_1; \mathcal{B}_3\}$ : The second basis reads explicitly

$$\mathcal{B}_3 = \left\{ |a, A\rangle, |a^\perp, A\rangle, |b, A^\perp\rangle, |b^\perp, A^\perp\rangle, |c, A^\perp\rangle, |c^\perp, A^\perp\rangle \right\}, \quad (59)$$

and suitable LETs map it to

$$\{|j_x, 0_x\rangle, |\hat{r}_\sigma j_x, 1_x\rangle, |\hat{r}_\tau j_x, 2_x\rangle\}, \quad (60)$$

which involve two rotations of the basis  $\{|j_x\rangle\}$  about the  $z$ -axis,  $\hat{r}_\sigma$  and  $\hat{r}_\tau$ . The operator  $\hat{U}$  in  $\mathcal{I}_1$  must be chosen such that  $\{|\hat{U}J_z\rangle\}$  is MU to the  $x$ -basis. All such  $U(3)$ -rotations are given by the two-parameter family

$$\hat{S}_{\zeta, \chi} = |0_x\rangle\langle 0_x| + e^{i\zeta}|1_x\rangle\langle 1_x| + e^{i\chi}|2_x\rangle\langle 2_x|, \quad (61)$$

diagonal in the  $x$ -basis, and defined in analogy to  $\hat{R}_{\xi, \eta}$  in Eq. (15). Altogether, we obtain a four-parameter family of MU product pairs,

$$\mathcal{P}_3 = \{|0_z, J_z\rangle, |1_z, \hat{S}_{\zeta, \chi} J_z\rangle; |j_x, 0_x\rangle, |\hat{r}_\sigma j_x, 1_x\rangle, |\hat{r}_\tau j_x, 2_x\rangle\}. \quad (62)$$

- $\{\mathcal{I}_3; \mathcal{B}_3\}$ : No pair results when we combine the product basis  $\mathcal{B}_3$  with  $\mathcal{I}_3$ . The standard transformations to simplify  $\mathcal{B}_3$  lead to

$$\left\{ |j_x, 0_x\rangle, |\hat{r}_\sigma j_x, 1_x\rangle, |\hat{r}_\tau j_x, 2_x\rangle \right\}, \quad (63)$$

since both the  $b$ -basis and the  $c$ -basis must be MU to the standard basis. The only basis MU to the three bases  $\{|j_x\rangle\}$ ,  $\{|\hat{r}_\sigma j_x\rangle\}$ , and  $\{|\hat{r}_\tau j_x\rangle\}$ , is the standard basis  $\{|j_z\rangle\}$ , which is also true for the case  $\{|\hat{r}_\sigma j_x\rangle\} = \{|\hat{r}_\tau j_x\rangle\}$ . Consequently, this would force the operators  $\hat{u}$  and  $\hat{v}$  to be the identity, in contradiction to the assumption that the three bases of  $\mathbb{C}^2$  present in  $\mathcal{I}_3$  do not coincide.

## C Appendix

Here we report a proof by A. Sudbery that the conditions of Eq. (56) in Appendix B are only satisfied if the bases in (at least) one pair coincide or all four bases are mutually unbiased. If  $\mathcal{B}_1$  and  $\mathcal{B}_2$  are orthonormal bases, we write  $\mathcal{B}_1 \mu \mathcal{B}_2$  to mean “ $\mathcal{B}_1$  and  $\mathcal{B}_2$  are mutually unbiased”.

**Theorem 5.** *Suppose  $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$  are orthonormal bases of  $\mathbb{C}^3$  satisfying*

$$\{\mathcal{B}_0, \mathcal{B}_1\} \mu \{\mathcal{B}_2, \mathcal{B}_3\}.$$

*Then either  $\mathcal{B}_0$  and  $\mathcal{B}_1$  are equivalent bases or  $\mathcal{B}_2$  and  $\mathcal{B}_3$  are equivalent bases or all four bases are mutually unbiased.*

Let  $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$  be represented by unitary matrices  $I, U, V, W$ , respectively, where we have chosen  $\mathcal{B}_0$  to be the standard basis of  $\mathbb{C}^3$ . We regard the bases  $U, UP$  and  $UD$ , with  $P$  a permutation matrix and  $D$  a diagonal, as equivalent bases. Note that if two orthonormal bases in  $\mathbb{C}^3$ , represented by unitary matrices  $U$  and  $V$ , are mutually unbiased, then  $U^\dagger V$  (where the dagger denotes hermitian conjugation) is a complex Hadamard matrix  $H$ . We can write any  $(3 \times 3)$  Hadamard matrix as

$$H = DFD' \text{ or } DF^\dagger D' \quad (64)$$

where  $D$  and  $D'$  are diagonal and  $F \equiv F_3$  is the Fourier matrix defined in Eq. (16). The condition  $\mathcal{B}_2 \mu \mathcal{B}_0$  implies the unitary  $V$  is a Hadamard matrix, and since  $F^\dagger = FP$ , the basis  $\mathcal{B}_2$  is equivalent to a basis represented by  $V = DF$ . Similarly,  $\mathcal{B}_3$  is equivalent to a basis represented by  $W = D'F$  where  $D'$  is diagonal. Now

$$\mathcal{B}_2 \mu \mathcal{B}_1 \implies V^\dagger U = KF^{(1)}L, \quad (65)$$

$$\mathcal{B}_3 \mu \mathcal{B}_1 \implies W^\dagger U = K'F^{(2)}L' \quad (66)$$

where  $K, L, K'$  and  $L'$  are diagonal and  $F^{(i)}$  is either  $F$  or  $F^\dagger$  ( $i = 1, 2$ ). Hence

$$U = DFKF^{(1)}L = D'FK'F^{(2)}L'. \quad (67)$$

We will now examine the relationship between  $U$  and the diagonal matrices  $D, K, L$  in the two cases  $U = DFKFL$  and  $U = DFKF^\dagger L$ , respectively. We can assume the leading entries of  $D$  and  $L$  to be  $d_{11} = l_{11} = 1$  by absorbing two phase factors in the diagonal matrix  $K$ .

**Lemma 4.** *Suppose  $U = DFKFL$  where  $D, K, L$  are diagonal unitary matrices with  $D = \text{diag}(1, \alpha, \beta)$ . Then either  $U = PE$  where  $P$  is a permutation matrix and  $E$  is diagonal, or the matrix elements of  $U$  are all non-zero and satisfy*

$$u_{12}u_{23}u_{31} = u_{13}u_{21}u_{32} = u_{11}u_{22}u_{33}, \quad (68)$$

and  $\alpha$  and  $\beta$  are given by

$$\alpha^3 = \frac{u_{21}u_{22}u_{23}}{u_{11}u_{12}u_{13}}, \quad (69)$$

$$\beta = \alpha^2 \frac{u_{12}u_{31}}{u_{21}u_{22}}. \quad (70)$$

Let  $K = \text{diag}(\gamma, \delta, \epsilon)$  and  $L = \text{diag}(1, \zeta, \eta)$ . Then

$$U = \begin{pmatrix} a & \zeta b & \eta c \\ \alpha b & \alpha \zeta c & \alpha \eta a \\ \beta c & \beta \zeta a & \beta \eta b \end{pmatrix} \quad (71)$$

where

$$\begin{aligned} a &= \frac{1}{3}(\gamma + \delta + \epsilon), \\ b &= \frac{1}{3}(\gamma + \omega\delta + \omega^2\epsilon), \\ c &= \frac{1}{3}(\gamma + \omega^2\delta + \omega\epsilon). \end{aligned} \tag{72}$$

Suppose one of  $a, b, c$  were zero, say  $a = 0$ . Then, since  $\gamma, \delta, \epsilon$  all have modulus 1, they must form an equilateral triangle in the complex plane, so either  $\delta = \omega\gamma$  and  $\epsilon = \omega^2\gamma$ , when  $b = 0$  and  $c = \gamma$ , or  $\delta = \omega^2\gamma$  and  $\epsilon = \omega\gamma$ , when  $b = \gamma$  and  $c = 0$ . In both cases  $U$  is of the form  $PE$ .

If none of  $a, b, c$  are zero, then all the matrix elements of  $U$  are non-zero and equations (68), (69) and (70) follow immediately from (71).

Exactly similar arguments prove

**Lemma 5.** *Suppose  $U = DFKF^\dagger L$  where  $D, K, L$  are as in Lemma 4. Then either  $U = PE$  where  $P$  is a permutation matrix and  $E$  is diagonal, or the matrix elements of  $U$  are all non-zero and satisfy*

$$u_{11}u_{23}u_{32} = u_{12}u_{21}u_{33} = u_{13}u_{22}u_{31}, \tag{73}$$

while  $\alpha$  is given by (69) and  $\beta$  by

$$\beta = \alpha^2 \frac{u_{13}u_{31}}{u_{21}u_{23}}. \tag{74}$$

We now return to eq. (67) and consider the four possibilities for  $(F^{(1)}, F^{(2)})$ .

**Case 1:**  $U = DFKFL = D'FK'FL'$ .

Let  $D = \text{diag}(1, \alpha, \beta)$ ,  $D' = \text{diag}(1, \alpha', \beta')$ . Then, by Lemma 4, either  $U$  is of the form  $PE$  (when the bases  $\mathcal{B}_0$  and  $\mathcal{B}_1$  are equivalent), or

$$\alpha^3 = \alpha'^3 \quad \text{and} \quad \frac{\beta'}{\beta} = \left(\frac{\alpha'}{\alpha}\right)^2. \tag{75}$$

Hence  $\alpha' = \alpha$  or  $\omega\alpha$  or  $\omega^2\alpha$ , so

$$D' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega\alpha & 0 \\ 0 & 0 & \omega^2\beta \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2\alpha & 0 \\ 0 & 0 & \omega\beta \end{pmatrix}. \tag{76}$$

This gives

$$V = DF = \begin{pmatrix} 1 & 1 & 1 \\ \alpha & \omega\alpha & \omega^2\alpha \\ \beta & \omega^2\beta & \omega\beta \end{pmatrix}, \quad (77)$$

$$W = D'F = \begin{pmatrix} 1 & 1 & 1 \\ \alpha & \omega\alpha & \omega^2\alpha \\ \beta & \omega^2\beta & \omega\beta \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 & 1 \\ \omega\alpha & \omega^2\alpha & \alpha \\ \omega^2\beta & \omega\beta & \beta \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 & 1 \\ \omega^2\alpha & \alpha & \omega\alpha \\ \omega\beta & \beta & \omega^2\beta \end{pmatrix}. \quad (78)$$

In each case the columns of  $W$  are a permutation of those of  $V$ . Thus either the bases  $\mathcal{B}_0$  and  $\mathcal{B}_1$  are equivalent or  $\mathcal{B}_2$  and  $\mathcal{B}_3$  are equivalent.

**Case 2:**  $U = DFKFL = D'FK'F^\dagger L'$ .

Suppose  $U$  is not of the form  $PE$ . Then both Lemmas 4 and 5 apply, and  $U$  has non-zero matrix elements satisfying (68) and (73). As in case 1, let  $D = \text{diag}(1, \alpha, \beta)$  and  $D' = \text{diag}(1, \alpha', \beta')$ . Now  $\alpha$  and  $\beta$  are given by Lemma 4, but  $\alpha'$  and  $\beta'$  are given by Lemma 5. Once again we have  $\alpha^3 = \alpha'^3$ , but now  $\beta'/\beta$  is not determined solely by  $\alpha'/\alpha$ :

$$\frac{\beta'}{\beta} = \left(\frac{\alpha'}{\alpha}\right)^2 \frac{u_{13}u_{22}}{u_{12}u_{23}}. \quad (79)$$

Using (68) and (73),

$$\begin{aligned} \left(\frac{u_{13}u_{22}}{u_{12}u_{23}}\right)^3 &= \left(\frac{u_{13}}{u_{12}}\right)^3 \left(\frac{u_{22}}{u_{23}}\right)^3 \\ &= \frac{u_{13}}{u_{12}} \cdot \frac{u_{23}u_{31}}{u_{21}u_{32}} \cdot \frac{u_{21}u_{33}}{u_{22}u_{31}} \cdot \frac{u_{22}}{u_{23}} \cdot \frac{u_{12}u_{31}}{u_{11}u_{33}} \cdot \frac{u_{11}u_{32}}{u_{13}u_{31}} \\ &= 1. \end{aligned} \quad (80)$$

Hence  $\alpha'/\alpha$  and  $\beta'/\beta$  are both cube roots of 1. Write  $\alpha' = \phi\alpha$ ,  $\beta' = \chi\beta$ . If  $\chi = \phi^2$  then, as shown in Case 1, the columns of  $V$  and  $W$  are the same, up to permutation, and the bases  $\mathcal{B}_2$  and  $\mathcal{B}_3$  are equivalent. If  $\chi \neq \phi^2$  then two of  $1, \chi, \phi$  are equal and the third is different. The same is true of the sets  $\{1, \omega\chi, \omega^2\phi\}$  and  $\{1, \omega^2\chi, \omega\phi\}$ . Hence the sums  $a = 1 + \chi + \phi$ ,  $b = 1 + \omega\chi + \omega^2\phi$  and  $c = 1 + \omega^2\chi + \omega\phi$  all have the same modulus. For  $\chi \neq \phi^2$ , the product

$$V^\dagger W = F^\dagger D^\dagger D' F = \frac{1}{3} \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}. \quad (81)$$

is a Hadamard matrix and hence the bases  $\mathcal{B}_2$  and  $\mathcal{B}_3$  are mutually unbiased. Thus in this case,  $\mathcal{B}_2$  and  $\mathcal{B}_3$  are either equivalent or mutually unbiased.

**Case 3:**  $U = DFKF^\dagger L = D'FK'FL'$ .

This is the same as Case 2 with  $V$  and  $W$  interchanged.

**Case 4:**  $U = DFKF^\dagger L = D'FK'F^\dagger L'$ .

This is similar to Case 1, using Lemma 5 instead of Lemma 4. The conclusion is the same.

We have now shown that in every case, either  $\mathcal{B}_2$  and  $\mathcal{B}_3$  are equivalent or  $\mathcal{B}_0$  and  $\mathcal{B}_1$  are equivalent or  $\mathcal{B}_2$  and  $\mathcal{B}_3$  are mutually unbiased. But the assumptions of the theorem are symmetric between the pairs  $\{\mathcal{B}_0, \mathcal{B}_1\}$  and  $\{\mathcal{B}_2, \mathcal{B}_3\}$ , so we can also prove that if  $\mathcal{B}_2$  is not equivalent to  $\mathcal{B}_3$  and  $\mathcal{B}_0$  is not equivalent to  $\mathcal{B}_1$ , then  $\mathcal{B}_0$  and  $\mathcal{B}_1$  are mutually unbiased and therefore all four bases are mutually unbiased.